DXing 2.4 GHz

By John Mayson

Many radio hobbyists enjoy DXing – that is, intercepting and identifying distant and exotic signals. Some of us search the bands below 500 kHz hunting for non-directional beacons (NDBs). Others monitor the mediumwave, FM, and television broadcast bands hunting for elusive signals. Scanner listeners find they can hear police and fire calls from distant states when conditions are right. So what's next for DXers? How about DXing 2.4 GHz?!

The Federal Communications Commission has assigned amateur, radiolocation, mobile satellite, radio determination satellite, mobile, and fixed radio services to the band between 2.4 and 2.5 GHz. Also sharing this swath of spectrum is the unlicensed Industrial, Scientific, and Medical (ISM) band. The Code of Federal Regulations Part 15 of Title 47 governs these unlicensed devices that include common household devices such as microwave ovens, cordless phones, and most importantly to us, the increasingly popular wireless computer networks. It is these networks that we will explore this month.

History

Radio-based computer networks are not a recent phenomenon. Amateur radio operators have used modes like RTTY and packet for some time. RTTY, or radio-teletype, isn't computerized *per se*, but it demonstrates sending data over radio. In 1971 the University of Hawaii created ALOHANET, the first wireless computer local area network (LAN).

ALOHANET came about after a Stanford University professor named Norm Abramson decided the surfing was better in Honolulu than in Palo Alto and joined the School of Engineering at the University of Hawaii. The system used 9600 baud modems and two 100 kHz bandwidth channels. The broadcast channel was 413.475 MHz and the random access channel was 407.350 MHz. An obvious question is why did they use two frequencies clearly in the federal government UHF band? The author can only guess that since the federal government (i.e., the Department of Defense) funds so much university research, the federal band was an obvious choice.

Over the years, computer networking protocols continued to evolve and by 1998 two wireless standards had surfaced. One was called Bluetooth. A consortium of communications companies that included Sweden-based Ericsson proposed the standard. Bluetooth was named after Harald Blåtand, a 10th century Viking king. "Blåtand" translates into "Bluetooth."

The second standard originated with the Institute of Electrical & Electronics Engineers (IEEE) and received the rather bland technical designation IEEE 802.11. Despite a name that would make marketing people cringe, IEEE 802.11 has become the wireless LAN standard in the United States and beyond. The wireless community has nicknamed the IEEE standard to something easier on the vocal cords, "WiFi", which is short for "wireless fidelity." At present time there are three "flavors" of WiFi available to the consumer market: 802.11a, 802.11b, and 802.11g (see table 1).

Equipment

While some higher end communications receivers will tune the ISM band (see table 2), they are totally useless when it comes to monitoring 802.11 networks. Mandatory equipment includes: a computer, a WiFi network card (preferably one with an external antenna jack), and packet sniffing software. Optional equipment includes: an external antenna and a GPS.

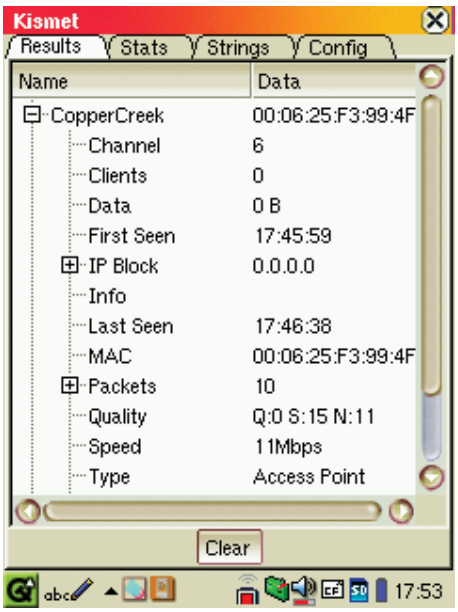
Table 2.

802.11 Wireless Frequencies

Ch.	Freq(GHz)		
1	2.412	2	2.417
3	2.422	4	2.427
5	2.432	6	2.437
7	2.442	8	2.447
9	2.452	10	2.457
11	2.462	12	2.467
13	2.472	14	2.484

The United States uses channels 1 through 11. Europe uses channels 1 through 13 except for France where only channels 10 through 13 are used. All 14 channels are used in Japan.

FCC regulations limit maximum output power of wireless devices to one watt. Most wireless equipment operates at a fraction of the power, some as low 20 milliwatts. This means you will have to travel to the signal rather than let the signal come to you. Therefore, when selecting a computer you should consider something that's portable such as a laptop or even a PDA. You do not need a high-end processor or a lot of memory.



QtKismet, a user friendly front end of kismet in action on a Sharp Zaurus.

Taking portable computer around town to monitor new networks is a hobby unto itself and is known as "wardriving." If you don't own a car you are free to "warwalk" or "warcycle." Despite the hawkish name, most folks who wardrive are peaceful people who don't wish harm on anyone. Twenty years ago, long before anyone had considered home wireless networks, we had another misunderstood hobby called "wardialing" where a person with a computer and a modem would dial every possible phone number in sequence looking for open systems. You can thank the 1983 movie *War Games* for the term. If you're too

Table 1.

Types of 802.11

At present time there are three 802.11 standards used in the consumer market: 802.11a, 802.11b, and 802.11g. Here are the differences between the three:

	802.11b	802.11a	802.11g
Popularity	Ready available	New technology	New, but expanding
Speed	11 Mb/s*	54 Mb/s	54 Mb/s
Cost	$	$$$	$$
Frequency	2.4 GHz	5 GHz	2.4 GHz
Indoor range	100 to 150 feet	25 to 75 feet	100 to 150 feet
Public access	Everywhere	None	Very little, but backwards compatible with 802.11b
Compatibility	"The Standard"	Incompatible with b and g	Compatible with b, not with a

young to remember the movie, a teenager played by Matthew Broderick almost started the Third World War while dialing around.

Whoa, is this legal?

Yes, as long as you remain within the bounds set in this article you are completely legal. Wardriving consists of passively monitoring the WiFi band and detecting information that is broadcast in the non-encrypted packets. If you attempt to gain access to an open network without first receiving authorization from the owner, then you have crossed the line and are on your own.

Isn't this considered hacking?

Yes and no. How's that for an answer? Soapbox please:

Hackers are accused of everything from releasing destructive computer viruses to shutting down power grids. I disagree. *Criminals* with computers release destructive computer viruses and shut down power grids. We don't refer to drug dealers as "pharmacists." We don't confuse counterfeiters with "artists" or "engravers."

Hacking is the art and science of discovery with computers. It has nothing to do with crime. Yes, some people commit crimes with computers, but hackers are not synonymous with criminals.

I will now return the soapbox. Thank you.

Back to the radio aspect

I promised the good folks at *Monitoring Times* this would be a radio-related article and not computer-related. But I first need to provide a basic overview of what it is we will be receiving and this requires a brief tutorial on 802.11.

Officially 802.11b provides a maximum bit rate of 11 Mb/s. In reality the maximum throughput is closer to 5.5 Mb/s. Why the discrepancy? 802.11 is not a very efficient protocol. All computer networks including 802.11 must broadcast more than just the data packets. The data packets need to know where they're going, where they originated, and other information beyond the scope of this article. Roughly 50% of the data passed over 802.11 is link layer overhead. Compare this to a cable modem where the overhead is around 10%.

Some 802.11 equipment vendors advertise 22 Mb/s speeds. Equipment such as this uses a proprietary chipset. While this is great for the average home user, if you do plan on wardriving, avoid such equipment. The packet sniffing software will not work with such a card. You, of course can, still detect and even access networks running at 22 MB/s even if your card only runs at 11 MB/s (you will operate at the lower speed). You just cannot use 22 Mb/s equipment to wardrive.

802.11 utilizes an encryption scheme known as "wired equivalent privacy" or WEP for short. WEP encrypts only the data packets and not the link layer packets. This means even while encrypted, an access point will still broadcast identification information such as the service set identifier (SSID) and media access control (MAC) address in the clear. These two pieces of information, in particular the MAC address, are key to identifying an access point.

An access point (AP) is simply the device that connects the Internet to the wireless world. Most home users connect their AP to their cable modem. They resemble very thin desktop scanners complete with an antenna, but no keypad. APs work right out of the box. This is a good and bad thing. It's good in that they're mindless to set up, but bad in that few users change their SSID, change the admin password, or enable WEP. Wardrivers frequently find SSIDs such as "default" or "linksys."

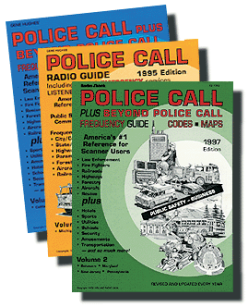
If a person did not bother to change their SSID, chances are they did not enable WEP or MAC address filtering, meaning anyone within range has access to their Internet connections. People with ill intent could introduce viruses or send hundreds of thousands of unsolicited commercial email messages with a nearly zero chance of being caught. Worse yet, some people are unknowingly hosting adult material or even illegal material on their hard drives through an open wireless LAN.

Every networking device in the world has a unique MAC address. This is a 12-character hex string usually written in the form 01:23:45:67:89:AB. Alert readers will note this provides 281,474,976,710,656 or over 281 trillion unique addresses. You can think of the MAC address as the call sign, something that will undoubtedly identify a particular AP. Yes, it is possible to spoof a MAC address, but for sake of this article we'll pretend everyone is honest.

Let's go wardriving

So far we have mentioned the computer

2004 POLICE CALL with U.S. CD-ROM!



Providing comprehensive frequency location and usage information, as well as radio signals, codes, trunking, maps, and jargon for law enforcement, fire fighters, rescue, federal agencies, forestry service, military bases and more. PLUS!!!! All the information from the seven-volume set packed into one powerful CD, searchable by any field with lightning-fast speed! The Police Call on CD features over a half million frequency listings in seven regional volumes! Including additional categories, you will be equipped to monitor police and fire, business and industry, hospital and ambulance, public utilities and transportation, sports and entertainment, aviation and railroads, and much more! And if you're monitoring trunking, this edition now includes talk group ID codes. A consolidated frequency list allows cross-referencing by frequency, with radio signals and ("ten") codes, FCC frequency allocations tables, an excellent chapter on technical scanner topics, and even a listener's glossary.

ORDER YOURS TODAY! Only $19.95 each! (Plus $3 UPS Ground shipping)

BOK21-04 - CT, ME, MA, NH, NY, RI, VT
BOK22-04 - DE, MD, NJ, PA
BOK23-04 - IL, IN, KY, MI, OH, WI
BOK25-04 - AZ, CO, ID, IA, KS, MN, MO, MT, NE, NV, NM, ND, SD, UT, WY
BOK26-04 - DC, FL, GA, NC, PR, SC, VA, WV
BOK27-04 - AL, AR, LA, MS, OK, TN, TX
BOK29-04 - CA, OR, WA

GROVE
800-438-8155
828-837-9200 fax: 828-837-2216
WWW.GROVE-ENT.COM
7540 Highway 64 West
Brasstown, NC 28902

(preferably a laptop or a PDA) and the wireless LAN card. The third item we need is software. The two most popular pieces of software is Netstumbler for Windows (**http://www.netstumbler.com**) and Kismet for Linux/Unix (**http://www.kismetwireless.net**). Before you go out and purchase any hardware, be sure to visit one of the two sites to verify which hardware will work with the software. And remember to avoid 22 Mb/s equipment. Both pieces of software are fairly straightforward to operate. What they do is scan across the appropriate frequencies (see table 2) and record pertinent information such as SSID, MAC address, channel, and whether WEP is enabled.

Can this get more boring?

In my experience wardriving was fun for about a day. Two things shocked me. One was how many APs in my community are wide open. The second is what people do use as SSIDs when they bother to change them. I've seen everything from physical addresses to words and phrases we can't print in this magazine.

My interest went from wardriving to this: How can ham radio operators and others interested in the radio hobby make use of what wardrivers have learned? What about an amateur radio only wireless LAN network in the 13-centimeter band (see table 3)?

Table 3. Amateur Radio 13 cm band.

13 Centimeters (2.3-2.31 and 2.39-2.45 GHz)	
2300-2302	Digital
2303.9-2304.2	QRP
2303.9-2304.1	CW
2304.1	National Calling frequency
2304.3-2403.4	Beacons
2304.5-2304.9	Crossband linear translators
2304.9-2305	Experimental beacons
2305-2306	FM Simplex
2305.2	FM Calling Frequency
2306-2309	Repeater inputs
2309-2310	Control & Auxiliary links
2390-2396	Television
2396-2399.5	Digital
2399.5-2400	Control & Auxiliary links
2400-2410	Satellites
2403-2408	Digital
2410-2413	Repeater outputs
2413-2418	Digital
2418-2430	Television
2430-2438	Satellites
2433-2438	Digital
2438-2450	Wide Band FX, TV, SS, etc.

Novice class:
1270-1295 MHz: CW, phone, Image, MCW, RTTY/Data (maximum power, 5 watts PEP)
All Amateurs except Novices:
1240-1300 MHz: CW, Phone, Image, MCW, RTTY/Data

Source: American Radio Relay League (ARRL)

And now the radio part!

Clever wardrivers incorporate a GPS into their setup. As they drive past an AP the software not only logs information broadcast by the AP, but also records the latitude and longitude. Various websites and wireless advocacy groups publish this information. This sounds like a useful way to test homebrew antennas and amplifiers! If you know the location and SSID of a particular AP, you can to attempt to detect them at great distances with homebrew equipment. Remember that "great distances" is a relative term here. 802.11 typically has the same range as a household cordless phone. A mile would easily be termed "a great distance."

A word on amplifiers. Do not build an amplifier to boost the output signal of your AP or wireless LAN card. If you do insist on doing this, do not operate it while in the United States of America. While the FCC allows external antennas, external amplifiers are illegal, even if they keep the signal under the legal limit of one watt. However, there's no law against boosting the signal into your receiver.

What I love the most about the radio hobby is how many sub-hobbies exist. One of my favorites is antenna design and construction. I have built my share of what appear to be broadband attenuators, but there's nothing quite like the thrill and sense of accomplishment of a homebrew antenna that actually works. Even more exciting is how easy antenna construction for 2.4 GHz can be. You can build a high gain antenna with very simple and readily available items: a coffee can, wire, washers, and the appropriate connector.

First I stop by the supermarket and buy a 39 ounce can of coffee. When I get home I open the can and dump the contents into the garbage because I don't drink coffee. Being the good ham radio geek that I am, I have N connectors on hand, but if I didn't, a visit to a local electronics store or mail order will get the correct parts into my hands.

Once I've collected all of the parts I point my web browser to **http://www.turnpoint.net/wireless/cantennahowto.html** to determine how to construct the antenna. If you're into antennas this is definitely the hobby for you! 2.4 GHz antennas are cheap and easy to construct.

In the United States we use WiFi channels 1 through 11, meaning the range of frequencies between 2.412 GHz and 2.462 GHz. Obviously the antenna should be tuned so the lower cut-off frequency is below 2.412 GHz and the higher cut-off frequency is above 2.462 GHz. If you're interested in only a particular channel you can select your can appropriately. Experiment!

The above mentioned website provides the guide wavelength in inches. The can itself should be 3/4 of the guide wavelength. It can be a little off. In general, longer cans will be more directional and provide higher gain than shorter cans (see figure 1).

Now drill or punch a hole with the center 1/4 of the guide wavelength from the bottom of the can. The hole should be the same diameter as your connector. Now the precision begins. Your piece of wire must stick out 1.21 inches from the connector (see figure 2). Few rulers are this accurate, but get as close as you can. Obviously, you can experiment with this length to see how it affects performance. Solder the wire in place and attach the connector to the can (see figure 3). Connect the connector to your wireless card and you're ready to go!

You will more than likely want to mount the "cantenna" to something. A camera tripod works well. If you're considering drilling into the can to attach a mounting bracket, keep in mind even a nut or a screw head can detune the antenna. Plastic tie-wraps work well for temporary setups.

Figure 1: All of these cans will work. Experiment and discover which one works best for you.

Figure 2: Connector with 1.21" wire attached.

Figure 3: Connector installed on a Pringles can.

A Pringles can antenna in action.

Fortunately for me, Intel named my hometown of Austin, Texas, as the third most "unwired" city in America. This means Austin is third behind Portland, Oregon, and the San Francisco Bay area for wireless access that is publicly available. Even if your hometown is not on Intel's list, you're not out of luck. If you have a Starbucks, chances are they host a T-

Mobile hotspot. T-Mobile is not free; however, you can passively detect to your heart's content.

Suppose I want to access the Austin Public Library's wireless LAN. First I know I have permission because their website says so. Next, I wardrive and verify the branch closest to me does in fact have WiFi and it is in use. (Free, publicly accessible WiFi networks too often go down and it can be days or even weeks before someone gets around to resetting them. Remember, these networks are free, so give them a break!) Your new antenna should work perfectly, but if the AP isn't on you will never know. Check the hotspot first.

Amateur Radio Applications

The 13-centimeter ham radio band overlaps the ISM band where we find WiFi devices. Once you have mastered building antennas out of beef stew cans you can work off some of those excess calories by climbing a mountain, or even a hill, with 13-centimeter ham gear and your homebrew antenna and start DXing.

It's alarming that the Internet search engine Google turns up nothing about 13-centimeter repeaters, but plenty of dire warnings about hams being in danger of losing this band to commercial interests. Get your local ham radio club involved in 13-centimeters! Every ham radio licensee, including novices, has at least some access to this band. Use it or lose it!

A company called 4ATV offers 13-centimeter band television equipment. Your local ham radio club could possibly install a "tower cam" giving hams in the area a bird's eye view of the community. Weather spotters could use it to watch for ominous weather without getting out of their seats.

A 13-centimeter voice repeater could be the answer to overcrowded 2-meter and 70-centimeter bands. Sure, there's not a whole lot of commercially available 13-centimeter equipment on the market, but isn't that why you became a ham? You enjoy the smell of solder in the morning!

Microwave links, packet networks, even satellite are all available to hams on the 13-centimeter band. If you're a ham and interested in 802.11 networks, I strongly encourage you to hop on the 13-centimeter bandwagon and save this spectrum for continued amateur radio use!

The 2.4 GHz band is far more crowded than 5 GHz, especially in residential settings where microwave ovens, cordless phones, and other wireless devices are the norm. Speed degrades with distance. Outdoor ranges can extend over a mile, perhaps farther with the right antenna. DX anyone?

* Some equipment manufacturers offer 22 Mb/s equipment. This does truly operate at the advertised speed and is backward compatible with 11 MB/s equipment, but cannot be used to wardrive due to the proprietary chipset used in 22 Mb/s equipment.

Table 4. Explanation of acronyms and terms.

AP	Access Point, the equipment connecting the Internet to the airwaves
DX	Long distance communications or radio monitoring
GHz	Gigahertz, equivalent to 1000 MHz
ISM	Industrial, Scientific, and Medical radio band
LAN	Local Area Network
MAC	Media Access Control, a unique 12-character hex identifier of a piece of network equipment
Mb/s	Megabits per second
SSID	Service Set Identifier
WAP	Wireless Access Point, another term for "AP"
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity, the common name for the 802.11 standard

Table 5. Web resources.

4ATV http://www.4atv.com/
Advisarial Science Laboratory http://www.adversarialsciencelab.net/newindex.html
Cantenna design http://www.turnpoint.net/wireless/cantennahowto.html
More cantenna design http://www.seattlewireless.net/index.cgi/DirectionalWaveguide
Defcon Wireless Shootout http://www.bluedonkey.org/wifi-shootout/
Intel's Most "Unwired" Cities http://www.intel.com/products/mobiletechnology/unwiredcities.htm
Kismet http://www.kissmetwireless.net
Netstumbler http://www.netstumbler.com
Wireless Guys http://www.wirelessguys.com
Wireless Node Database Project http://www.locfinder.com/

SCANNER USERS • COMMUNICATIONS PROFESSIONALS

Buy Police Call 2004 and get a CD at no extra cost!

POLICE CALL
2004 EDITION

COMPLETELY REVISED THROUGH JULY, 2003

- With Fully Searchable Nationwide CD.
- 20,000 Codes and Signals.
- Trunking Talkgroup IDs.
- Includes U.S. Government, Rail & Air.
- Illustrated 10-Page Listener's Guide.

GOT A SCANNER? GET POLICE CALL

At your scanner dealer and all Radio Shack stores.
Visit our web site at www.policecall.com

*More People Buy **POLICE CALL** Than All Other Frequency Guides (VHF/UHF) Combined.*